Claims 1-18, 32-49 and 63-78

Independent claim 1 recites a method for determining whether a client communication system seeking access to a host communication system is authorized to do so. The method includes performing a mathematical computation on an access password and a client-communication-system-specific identifier and designating a client communication system as unauthorized based on a result of the mathematical computation. The client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

1. Cane does not describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

In contrast, Cane describes techniques for "locking" personal computer software that is distributed on CD-ROM or over a network, where the "locking" prevents total or partial access to the software by a user who has not purchased the software, and later "unlocking" the software once the user purchases the software. See Cane at col. 3, lines 21-38. To enable such locking, Cane discloses encrypting software and storing, in a table (called a "software-encryption key table" or a "software-key table"), a software identifier associated with the software encryption key used to encrypt the software. See Cane at col. 5, lines 28-30 and col. 6, lines 17-29. The software-key table is used to identify the software encryption key that had been used to encrypt the particular software that is to be unlocked for installation and use by a purchaser. See Cane at col. 6, lines 24-29 and col. 3, lines 28-35.

Cane also discloses a personal computer decryption device (referred to as a "PCDD") that is included in a computer on which the software is to be installed and used. See Cane at col. 4, line 8-14 and FIG. 1. The personal computer decryption device stores a hardware identifier and a password key. See Cane at col. 4, lines 15-22, and FIG. 2. The personal computer decryption device is used to decrypt the software so that the software can be installed and used on the computer in which the personal computer decryption device resides. See Cane at col. 3, lines 35-38, and col. 4, lines 1-2, 26-37.

Notably, Cane indicates that, in a preferred embodiment, the password key bears "no algorithmic relationship to the hardware identifier." See Cane at col. 4, lines 22-25 (emphasis

added). Cane uses a table (called a "hardware-password key table" or a "serial number-key table") to store the association of a hardware identifier and the password key that both are stored on a personal computer decryption device. See Cane at col. 5, lines 25-30, and col. 6, lines 18-32. Cane's serial number-key table is later used to determine a password key that corresponds to a particular hardware identifier. See Cane at col. 3, lines 22-25; col. 5, lines 25-30; and col. 6, lines 18-32.

In general, Cane's process for unlocking software includes generating an encrypted password that is sent to the user's computer and using the personal computer decryption device of the user's computer to decrypt the password, which is then used to decrypt and "unlock" the software. See Cane at col. 3, lines 28-38 and col. 4, lines 27-36. See also Cane at FIG. 4 (illustrating a flow diagram of a preferred environment in which a software vendor 400 provides encrypted software to a publishing center 401, which, in turn, provides encryption key and software identifier information to an order center 402, which provides a user 404 with a password to unlock the software after purchase) and col. 5, lines 19-43 (describing the flow between the entities of FIG. 4).

More particularly, Cane's process for unlocking software includes generating a password using a software encryption key and a password key. See Cane at col. 6, lines 31-38 and col. 7, lines 64-67. See also Cane at col. 4, lines 27-36. The particular software encryption key to be used corresponds to the software to be unlocked and is determined by looking up, in the software-key table, the software identifier of the software to be unlocked. See Cane at col. 6, lines 31-34 and col. 4, lines 27-34. The particular password key to be used corresponds to the password key stored on the personal computer decryption device of the computer on which the software to be unlocked resides, and the particular password key is determined by looking up, in the serial number-key table, the hardware identifier stored in the personal computer decryption device. See Cane at col. 6, lines 31-34 and col. 4, lines 27-34. Presumably, the software encryption key is encrypted with the password key. In any event, the encrypted password is sent to the user's computer, and the personal computer decryption device decrypts, using its stored password key, the password, which "recovers" the software encryption key. See Cane at col. 5, lines 5-7 and col. 6, lines 45-53. The software encryption key then is used to decrypt the software. See Cane at col. 6, lines 54-58.

As such, Cane discloses a password that is generated based on a software encryption key and a password key, neither of which being specific to the client communication system used to store data to be unlocked by these keys. Moreover, the software encryption key is a cryptographic key that is used to encrypt and decrypt the software, and, hence, the software encryption key is not a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system, as recited in independent claim 1. The password key is a cryptographic key that is used to encrypt and decrypt the generated password, and, hence, the password key is not a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system, as recited in independent claim 1.

Moreover, while Cane discloses that the hardware identifier of a particular personal computer decryption device is looked-up using the serial number-key table identifier to determine the password key stored on the personal computer decryption device, Cane does not describe or suggest encrypting, decrypting or otherwise performing a computation on a hardware identifier stored in a personal computer decryption device.

In addition, the Office action also asserts that an algorithm is equivalent to a mathematical computation. See Office Action of July 21, 2005 at page 2 (stating "...to perform a mathematical computation (*i.e.* algorithm") and citing "Cane, algorithm") (emphasis added). Applicant respectfully disagrees that disclosure of the term algorithm is tantamount to disclosure of a mathematical computation. Moreover, as described above, Cane does not describe or suggest performing a mathematical computation on a hardware identifier stored in a personal computer decryption device. As such, Cane does not describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system, as required by independent claim 1.

In another aspect, Cane discloses decrypting, using the password key, an authorization code associated with the software and using the decrypted authorization code to trigger the generation of a message digest that is used to authorize the running of previously decrypted

software. See Cane at col. 6, line 59 to col. 7, line 37. This aspect of Cane also does not describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system. Nor does the Office action contend that this portion of Cane does so.

Accordingly, Cane does not describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system, as recited in independent claim 1. Because Cane does not perform the claimed mathematical computation, Cane necessarily cannot describe or suggest designating a client communication system as unauthorized based on a result of the claimed mathematical computation, also as recited in independent claim 1.

As noted by the Office action, Cane does not disclose a client-communication-system-specific identifier being derived from information that identifies at least a hardware component or aspect of the client communication system, as recited in independent claim 1. See Office action of December 12, 2005 at page 3. For this deficiency, the Office action relies on Kataoka.

2. Kataoka does not remedy Cane's failure to describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

Kataoka, however, is directed to a security system for protecting information stored in portable storage media by validating identifiers written in the storage media and only permitting qualified terminals to retrieve and decode data that has been encrypted and stored on the storage media. See Kataoka at col. 1, lines 9-12 and lines 55-58. To do so, in general, the security system of Kataoka includes an individual identifier, a terminal identifier, and security control means. See Kataoka at col. 1, lines 59-63. The individual identifier is an identifier previously written into the storage medium, the terminal identifier is an identifier uniquely assigned to a terminal, and the security control means permits the terminal to access the data in the storage medium only when the individual identifier extracted from the storage medium and the terminal

identifier extracted from the terminal are both valid. See Kataoka at col. 1, line 64 to col. 2, line 3.

The Office action indicates that Kataoka's terminal ID corresponds to the claimed client-communication-system-specific identifier that is derived from information that identifies at least a hardware component or aspect of the client communication system. See Office action of December 12, 2005 at page 3, lines 7-8 (stating "terminal ID (or client communication system specific identifier)"). Even assuming for the sake of argument only that the Kataoka's terminal ID corresponds to the claimed client-communication-system-specific identifier, Kataoka does not remedy Cane's failure to describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system.

In general, the terminal ID of Kataoka is uniquely identifies a particular terminal and is used to limit access to storage medium that has been previously associated with the particular terminal. See Kataoka at col. 4, lines 32-34. More particularly, Kataoka discloses an association process in which a particular terminal ID is written to the storage medium and the written terminal ID is later used to limit access to the storage medium based on a correspondence between the terminal ID written to the storage medium in the association process and the identifier of the terminal being used. See Kataoka at col. 4, lines 37-54; col. 5, lines 11-27 and 51-57. However, Kataoka appears to be silent as to how the identifier of the terminal is determined. Moreover, Kataoka discloses that "each terminal in the branch office is uniquely identified with its unit number, which can be used as a terminal ID." Kataoka at col. 4, lines 43-45. Notably, during the association process in which the terminal ID is written to the storage medium to be associated with a particular terminal, Kataoka's terminal ID is determined by a person – that is, "[a]n administrator in a branch office determines an identifier of a specific terminal that is exclusively allowed to read and write that storage medium [and] the security system accepts the terminal ID determined by the administrator.... The terminal ID is written into the authorized storage medium to give an exclusive read/write access privilege to the terminal." Kataoka at col. 4, lines 41-54.

To determine if the identifiers are valid, Kataoka appears to consult an authorization table. See Kataoka at col. 3, lines 53-56 and Fig. 1, element 3. In any event, Kataoka does not

describe performing a mathematical computation on the identifiers, nor does the Office action contend that Kataoka does so.

Therefore, Kataoka does not describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system, as recited in independent claim 1.

3. One skilled in the art would not have been motivated to combine Kataoka with Cane.

Moreover, Kataoka's process of checking whether identifiers are valid by consulting an authorization look-up table before permitting access to storage media cannot be properly combined with Cane's personal decryption device. One skilled in the art would not have been motivated by the media access protection system of Kataoka with Cane's personal decryption device to protect against unauthorized use of software that had not been purchased. Nothing in Kataoka or Cane would have provided motivation to incorporate Kataoka's validation of a terminal identifier with Cane's personal decryption device. Contrary to assertions made in the rejection, to provide a demand for more reliable security system to protect information in storage media from unauthorized access and ensure safe delivery, is not sufficient motivation for combining Kataoka with Cane. Stated differently, even if one were motivated to provide a demand for more reliable security system to protect information in storage media from unauthorized access and ensure safe delivery, such motivation would not inspire a combination of Kataoka with Cane. Nor does the mere existence of a terminal identifier that is used to limit access to storage media provide motivation to incorporate Kataoka's terminal identifier with Cane's personal decryption device. Moreover, while Kataoka describes using a terminal identifier to limit access to storage media, limiting access to storage media is not limiting access to a host communication system.

As such, Kataoka does not remedy Cane's failure to describe or suggest performing a mathematical computation on an access password and a client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system, as recited in independent claim 1.

Accordingly, neither Cane, Kataoka, nor any proper combination of the references, describes or suggests performing a mathematical computation on an access password and client-communication-system-specific identifier, where the client-communication-system-specific identifier is derived from information that identifies at least a hardware component or aspect of the client communication system, as recited in independent claim 1. Because neither Cane, Kataoka, nor any proper combination of the references, describes or suggests performing a mathematical computation as recited in independent claim 1, the references necessarily do not describe or suggest designating a client communication system as unauthorized based on a result of the mathematical computation, also as recited in independent claim 1.

For at least these reasons, applicant respectfully requests withdrawal of the rejection of independent claim 1, along with claims 2-18 that depend therefrom.

Independent claim 32 recites a computer readable medium or propagated signal having embodied thereon a computer program for identifying an unauthorized client communication system seeking access to a host communication system in a manner corresponding to that of independent claim 1, and independent claim 63 recites an apparatus that does the same.

Accordingly, for at least the reasons noted above with respect to independent claim 1, applicant requests withdrawal of the rejection of independent claims 32 and 63, along with claims 33-49 and claims 64-78 that depend therefrom.

Claims 19-31, 50-62 and 79-92

Independent claim 19 recites a method for handling information about an authorized client communication system. The method includes, *inter alia*, performing a mathematical computation on an access password and a client-communication-system-specific identifier.

Accordingly, for at least the reasons noted above with respect to independent claim 1, applicant requests withdrawal of the rejection of independent claims 19, along with claims 20-31 that depend therefrom.

Independent claim 50 recites a computer readable medium or propagated signal having embodied thereon a computer program for handling information about an authorized client communication system in a manner corresponding to that of independent claim 19, and independent claim 79 recites an apparatus that does the same.

Accordingly, for at least the reasons noted above with respect to independent claim 1, applicant requests withdrawal of the rejection of independent claims 50 and 79, along with claims 51-62 and 81-92 that depend therefrom.

Request for Initialed PTO-1449

As an administrative matter, applicant notes the Office action of December 12, 2005 did not include an initialed copy of the Form PTO-1449 filed on June 28, 2005. It is therefore respectfully requested that the Examiner return to the applicant a copy of the Form PTO-1449 with the Examiner's initials indicating that each of the references was considered. For the Examiner's convenience, a courtesy copy of the Form PTO-1449 filed on June 28, 2005 is included.

Conclusion

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this reply should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this reply, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicant submits that all claims are in condition for allowance.

Applicant notes that February 12, 2006 fell on a Sunday. No fee is believed due. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: February 13, 2006

Barbara A. Benoit
Reg. No. 54,777

Customer No.: 26171
Fish & Richardson P.C.
1425 K Street, N.W., 11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331